UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/728,302	12/04/2003	Brian Francis Cox	112025-0530	7927

24267 7590 01/09/2009

CESARI AND MCKENNA, LLP
88 BLACK FALCON AVENUE
BOSTON, MA 02210

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
01/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/728,302	COX ET AL.	
	Examiner	Art Unit	
	Christian LaForgia	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 April 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 31 October 2008 has been entered.

2. Claims 1-32 have been presented for examination.

Response to Arguments

3. Applicant's arguments with respect to claims 1-32 have been considered but are moot in view of the new grounds of rejection set forth below.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-4, 8, 14, 18, 21, 24 and 29-32 are rejected under 35 U.S.C. 102(a) and 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2003/0152067 A1 to Richmond et al., hereinafter Richmond

6. As per claims 1, 14, 18, and 24, Richmond teaches a method, an intermediate node, an apparatus, and a computer-readable medium for implementing port-based network access control at a shared media port in an intermediate node, the shard media port being a physical interface coupled to a plurality of client nodes, the method comprising:

partitioning the shared media port into a plurality of logical subinterfaces, wherein a logical subinterface is a logical division of a physical interface (Figure 1A [element 118], paragraphs 0014, 0023, i.e. dividing a port into one or more virtual ports), each logical subinterface dedicated to providing access to a different network or subnetwork accessible through the intermediate node (Figure 1A [element 116], paragraph 0023, i.e. network entry device permits access to internal devices);

receiving a data packet at the shared media port from a first client node (Figure 15 [element 1502], paragraph 0273, i.e. receiving a packet);

associating the received data packet with a first logical subinterface in the plurality of logical subinterfaces (paragraph 0263, i.e. configuring an individual virtual port according to an identity of a user);

determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork (Figure 15 [element 1506], paragraphs 0274-0277, i.e. performing authentication according to 802.1X, RADIUS, a NOS, etc.);

if the first client node is determined to be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork, forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork (paragraphs 0029, 0274-0277, 0279, 282);

receiving a second data packet at the shard media port from a second client node (Figures 1A [118], 15 [element 1502], paragraphs 0023, 0273, i.e. receiving a packet from one of the multiple users connected through the entry port module);

associating the second received data packet with the first logical subinterface (paragraphs 0023, 0263, i.e. configuring an individual virtual port according to an identity of a user, wherein there are multiple users via the entry port module);

determining whether the second client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork (Figure 15 [element 1506], paragraphs 0274-0277, i.e. performing authentication according to 802.1X, RADIUS, a NOS, etc); and

if the second client node is determined to not be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork, preventing the second received data packet from being forwarded over the first logical subinterface's dedicated network or subnetwork, while still allowing data packets from the first client node to be forwarded if the first client node is determined to be authenticated (paragraphs 0029, 0274-0277, 0279, 282, 287, if the virtual port is configured for a user, than a user failing authentication on a single virtual port would have no bearing on users on other virtual ports).

7. Regarding claims 2 and 30, Richmond teaches performing at least one of dropping the received data packet or reclassifying the received data packet to a different logical subinterface, if the first client node is determined not to be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork (paragraphs 0010, 0127, 0157, 0159, 0166, 0281).

8. Regarding claims 3, 27, and 31, Richmond teaches wherein the first logical subinterface's dedicated network or subnetwork is a virtual private network (VPN) (paragraph 0036).

9. Regarding claims 4, 28, and 32, Richmond teaches wherein a logical subinterface in the plurality of logical subinterfaces is dedicated to providing access to the Internet (paragraphs 0018, 0024, 0035, 0036, 0130).

10. Regarding claims 8 and 21, Richmond teaches wherein the step of associating the received data packet with the first logical subinterface, further comprises locating an entry in a routing table configured to store routing information associated with the received data packet; and associating the received data packet with the first logical subinterface based on the contents of the routing-table entry (paragraphs 0029, 0274-0277, 0279, 282, 287).

11. As per claim 29, Richmond teaches a method for implementing port-based network access control at a shared media port in an intermediate node, the shared media port being a physical interface coupled to a plurality of client nodes, the method comprising:

partitioning the shared media port into a plurality of logical subinterfaces by logically dividing the shared media port into subinterfaces (Figure 1A [element 118], paragraphs 0014, 0023, i.e. dividing a port into one or more virtual ports), each logical subinterface dedicated to providing access to a different network or subnetwork accessible through the intermediate node

(Figure 1A [element 116], paragraph 0023, i.e. network entry device permits access to internal devices);

receiving a data packet at the shared media port from a first client node (Figure 15 [element 1502], paragraph 0273, i.e. receiving a packet);

associating the received data packet with a first logical subinterface in the plurality of logical subinterfaces (paragraph 0263, i.e. configuring an individual virtual port according to an identity of a use);

determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork (Figure 15 [element 1506], paragraphs 0274-0277, i.e. performing authentication according to 802.1X, RADIUS, a NOS, etc.); and

if the first client node is determined to be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork, forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork (paragraphs 0029, 0274-0277, 0279, 282).

Claim Rejections - 35 USC § 103

12. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

13. Claims 5, 9, 11, 15, 17, 19, 22, 23, and 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richmond in view of U.S. Patent Application Publication No. 2005/0055570 A1 to Kwan et al., hereinafter Kwan.

14. Regarding claims 5, 17, and 19, Richmond does not teach wherein the step of determining whether the first client node is authenticated to communicate over the first logical

subinterface's dedicated network or subnetwork further comprises parsing a source media access control (MAC) address from the received data packet; comparing MAC address and 802.1X formats with stored known Ethernet and authentication packet types; identifying an authentication state stored in the indexed MAC-filter entry; and determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork based on the stored authentication state stored in the indexed MAC-filter entry.

15. Kwan teaches wherein the step of determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork further comprises:

parsing a source media access control (MAC) address from the received data packet (Figure 3 [block 304], paragraphs 0039, 0046-0049);

comparing MAC address and 802.1X formats with stored known Ethernet and authentication packet types (Figure 3 [block 306], paragraphs 0039, 0046);

identifying an authentication state stored in the indexed MAC-filter entry (paragraphs 0012, 0039, 0046, i.e. determining if the MAC address are secure); and

determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork based on the stored authentication state stored in the indexed MAC-filter entry (Figure 3 [block 310], paragraphs 0040).

16. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the MAC filtering at the network entry device, since Kwan states at

paragraph 0014 that providing MAC authentication provides network security in a more efficient manner.

17. Regarding claims 9, 15, and 22, Richmond does not teach receiving an authentication request from the first client node at the shared media port; in response to receiving the authentication request, creating a MAC filter associated with the shared media port if the MAC filter has not already been created; copying a source MAC address stored in the received authentication request into an appropriate entry in the MAC filter; forwarding the received authentication request to an authentication service; receiving a response from the authentication service, the response identifying an authentication state associated with the first client node; and storing the authentication state into the same MAC filter entry into which the source MAC address was copied.

18. Kwan teaches receiving an authentication request from the first client node at the shared media port (Figure 4, paragraph 0050);

in response to receiving the authentication request, creating a MAC filter associated with the shared media port if the MAC filter has not already been created (paragraphs 0055-0057, i.e. learn secure MAC addresses);

copying a source MAC address stored in the received authentication request into an appropriate entry in the MAC filter (paragraphs 0055-0057, i.e. storing a list of the secure MAC addresses);

forwarding the received authentication request to an authentication service (paragraphs 0055-0057, 0070-0076);

receiving a response from the authentication service, the response identifying an authentication state associated with the first client node (paragraphs 0055-0057, 0070-0076); and

storing the authentication state into the same MAC filter entry into which the source MAC address was copied (paragraphs 0055-0057, 0070-0076, i.e. storing a list of the secure MAC addresses).

19. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the MAC filtering at the network entry device, since Kwan states at paragraph 0014 that providing MAC authentication provides network security in a more efficient manner.

20. With regards to claims 11 and 23, Richmond teaches wherein the received authentication request is an 802.1X authentication request (paragraphs 0274-0277).

21. As per claim 25, Richmond teaches an apparatus comprising:

a shared media port that is a physical interface and has a trusted subinterface configured to provide access to a trusted network or subnetwork and an untrusted subinterface configured to provide access to an untrusted network or subnetwork, wherein a subinterface is a logical divide of a physical interface (Figure 1A [element 118], paragraphs 0014, 0023, i.e. dividing a port into one or more virtual ports; as noted, Richmond discloses 802.1X authentication which the prior art has shown both trusted and untrusted ports);

an authenticator configured to receive authentication requests from a plurality of client nodes and in response the authentication requests to independently assign to each of the plurality

of client nodes an authentication state (Figure 15B [element 1506], paragraphs 0208-210, 0272, 0274-0277, 0278).

22. Richmond does not disclose a media access control (MAC) filter configured to maintain an entry for each client node indicating the authentication state of the client node and a MAC address of the client node, and in response to receipt of a data packet from a particular client node directed to the trusted subinterface, to index to an entry of the MAC filter based on a source MAC address of the data packet, to identify the authentication state of the particular client node stored in the indexed MAC-filter entry, and to determine whether the particular client node is authenticated to communicate over the trusted subinterface, and if so, to permit the particular client node to access the trusted subinterface, wherein the media access control (MAC) filter grants client nodes access on a client by client basis.

23. Kwan teaches a media access control (MAC) filter (paragraph 0064) configured to maintain an entry for each client node indicating the authentication state of the client node and a MAC address of the client node, and in response to receipt of a data packet from a particular client node directed to the trusted subinterface, to index to an entry of the MAC filter based on a source MAC address of the data packet, to identify the authentication state of the particular client node stored in the indexed MAC-filter entry, and to determine whether the particular client node is authenticated to communicate over the trusted subinterface, and if so, to permit the particular client node to access the trusted subinterface (paragraphs 0039-0044, 0064),

wherein the media access control (MAC) filter grants client nodes access on a client by client basis (paragraph 0081, i.e. network access device **602** can selectively accept packets from

user devices having valid MAC addresses while dropping packets from user devices having invalid MAC addresses).

24. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the MAC filtering at the network entry device, since Kwan states at paragraph 0014 that providing MAC authentication provides network security in a more efficient manner.

25. Regarding claim 26, Kwan teaches wherein the MAC filter is further configured to redirect a data packet of the particular client node form the trusted subinterface to the untrusted subitnerface if the particular client node is not authenticated to communicate over the trusted subinterface (paragraphs 0015, 0016, 0039, i.e. packets or frames are redirected to another network destination).

26. Claims 6 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richmond in view of Kwan, and in further view of U.S. Patent Application Publication No. 2005/0177865 to Ng et al., hereinafter Ng.

27. With regards to claim 6, Kwan does not teach wherein the MAC filter is organized as a hash table.

28. Ng discloses wherein the state information has been stored using a hash function (paragraph [0080]).

29. It would have been obvious to one of ordinary skill in the art at the time the invention was made to organize the MAC filter as a hash table, since one of ordinary skill in the art would

recognize that the MAC addresses were being used as authentication means it would be necessary to store the address in a protected format, similar to how Unix systems store user passwords in a hashed filed, to prevent unauthorized users from acquiring the MAC addresses if the intermediate node was ever compromised.

30. With regards to claim 10, Kwan teaches indexing an entry in the MAC filter and storing the MAC address at the filter entry (paragraphs 0055-0057, i.e. storing a list of secure MAC addresses).

31. Richmond and Kwan do not teach wherein the MAC address are hashed prior to being indexed.

32. Ng discloses wherein the state information has been stored using a hash function (paragraph [0080]).

33. It would have been obvious to one of ordinary skill in the art at the time the invention was made to organize the MAC filter as a hash table, since one of ordinary skill in the art would recognize that the MAC addresses were being used as authentication means it would be necessary to store the address in a protected format, similar to how Unix systems store user passwords in a hashed filed, to prevent unauthorized users from acquiring the MAC addresses if the intermediate node was ever compromised.

34. Claims 7, 16, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richmond in view of Kwan, and in further view of U.S. Patent Application No. 2004/0208151 to Haverinen et al., hereinafter Haverinen.

35. Regarding claims 7, 16, and 20, Kwan teaches parsing a destination address from the received data packet (paragraphs 0032, 0034);

comparing the parsed destination address to one or more addresses stored in a filter associated with the shared media port (paragraphs 0032, 0034); and

if the parsed destination address matches an address stored in the filter, forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork, even if the first client node is determined not to be authenticated to communicate over that network or subnetwork (paragraphs 0032, 0034).

36. Kwan and Richmond do not teach wherein the destination address is an IP address.

37. Haverinen discloses using an IP address to authentication data (paragraph 0029).

38. It would have been obvious to one of ordinary skill in the art at the time the invention was made to perform an open systems authentication protocol using the destination IP address, since Haverinen states at paragraph [0004] that using an open systems authentication protocol, specifically one focused on the third layer of the OSI model, allows wireless users to authenticate and access network resources, thereby allowing users the freedom to access network resource whenever and where ever they would like. This is further supported by paragraph 0034 of Kwan, which includes the option for layer 3 and network layer functions of the OSI model.

39. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Richmond in view of Kwan, and in further view of U.S. Patent No. 6,891,819 to Inoue et al., hereinafter Inoue.

40. With regards to claim 12, Richmond and Kwan do not teach sending an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node fails to authenticate at the shared media port a predetermined number of times.

41. Inoue discloses tracking the number of times a user has failed authentication and providing an indication that said account has failed authentication a predetermined number of times (Figures 12-14, 18 and 19, column 12, lines 45-67, column 13, lines 22-46, column 17, lines 53-59).

42. It would have been obvious to one of ordinary skill in the art at the time the invention was made to send an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node fails to authenticate at the shared media port a predetermined number of times, since Inoue states at column 3, lines 1-6 that tracking the number an authentication fails helps to prevent the improper acquisition of user or network information since reaching the threshold of improper authorization attempts is a clear indicator that the user account or mobile system has been compromised.

43. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Richmond in view of Kwan, and in further view of U.S. Patent Application Publication No. 2004/0158735 to Roese, hereinafter Roese.

44. With regards to claim 13, Richmond and Kwan do not teach sending an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node's authentication state changes from an authenticated state to an unauthenticated or unknown state.

45. Roese teaches sending an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node's authentication state changes from an authenticated state to an unauthenticated or unknown state (paragraph [0029], i.e. tracking state changes via a tracking function).

46. It would have been obvious to one of ordinary skill in the art at the time the invention was made to send an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node's authentication state changes from an authenticated state to an unauthenticated or unknown state, since one of ordinary skill in the art would recognize that it would serve as an alert to an administrator that potential malicious behavior is occurring.

Conclusion

47. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

48. The following patents are cited to further show the state of the art with respect to 802.1X authentication, such as:

United States Patent Application Publication No. 2003/0154380 A1 to Richmond et al., which is cited to show a related co-pending application.

United States Patent No. 6,990,592 B2 to Richmond et al., which is cited to show a related patent.

49. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

50. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

51. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

clf